JAP:JMH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - -X

16 M 0162

UNITED STATES OF AMERICA

- against -

CHRISTOPHER ARROYO,

Defendant.

- - - - - - - - - - - - - - - - -X

COMPLAINT

(18 U.S.C. §§ 875(d), 2252(a)(2))

EASTERN DISTRICT OF NEW YORK, SS:

STACY SHAHRANI, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

On or about and between 2012 and 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant CHRISTOPHER ARROYO did knowingly receive and distribute any visual depiction, the production of such visual depiction having involved the use of one or more minors engaging in sexually explicit conduct and such visual depiction was of such conduct, using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported, by any means including by computer.

(Title 18, United States Code, Section 2252(a)(2)).

On or about and between 2013 and 2015, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant

CHRISTOPHER ARROYO did, with intent to extort from any person, any money or other thing of value, transmit in interstate or foreign commerce communications containing threats to injure the property or reputation of the addressee.

(Title 18, United States Code, Section 875(d)).

The source of your deponent's information and the grounds for her belief are as follows:[1]

1. I have been a Special Agent with the FBI since December 2008 and am currently assigned to the New York Office. Since July 2013, I have been assigned to a Crimes Against Children squad and have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed thousands of photographs depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

2. I am familiar with the facts and circumstances of this investigation from, among other sources, my own personal participation in the investigation, my review of

---

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

3. On February 25, 2016, FBI agents executed a search warrant, issued on February 22, 2016, by the Honorable Steven M. Gold, at the defendant CHRISTOPHER ARROYO's residence, located at 10520 66th Avenue, Apartment 6A, Forest Hills, New York ("the Forest Hills Address").

4. The facts in support of the application for the search warrant, in sum and substance, relate to CHRISTOPHER ARROYO's internet communications with a female minor born on June 4, 2000, whose initials are A.C. As set forth in the affidavit in support of the application for the search warrant, between approximately 2012 and 2015, ARROYO requested and received approximately 15 digital images over the Internet from A.C. depicting her in various stages of undress, including pictures of her masturbating.

5. ARROYO further threatened to post one or more of these images of A.C. publically on the Internet if A.C. terminated her relationship with ARROYO.

6. The affidavit in support of the application for the search warrant, and the warrant itself, were filed under docket number 16-MJ-144, and are attached hereto as Exhibit A, and the facts state din that affidavit are incorporated herein.

7. Along with other FBI agents, I executed the search warrant at the Forest Hills Address on the morning of February 25, 2016. When we arrived at the Forest Hills Address, we announced ourselves as law enforcement officers and knocked on the door, which was ajar. We then entered the Forest Hills Address and secured the location.

8. Present at the Forest Hills Address were several family relatives of the defendant CHRISTOPHER ARROYO. FBI agents advised that they were present to execute the search warrant and provided a copy of the warrant to review. ARROYO was not present.

9. FBI agents searched the Forest Hills Address based on the warrant. FBI agents located a 64-gigabyte PNY-brand USB thumb-drive ("the Thumb-drive") in a set of drawers next to a bed identified by the defendant's brother as belonging to the defendant.

10. FBI agents performed a preliminary forensic review of the contents of the Thumb-drive. Located within a folder titled with A.C.'s first name and the word "slut," FBI agents located numerous photographs depicting an individual who appears to be A.C. Located within a folder titled with A.C's first name and the word "pictures," FBI agents located numerous photographs depicting an individual who appears to be A.C. One image in this folder depicts a female from behind, with her vagina and buttocks spread apart in a lewd and lascivious manner. The female's hair is visible, and the hair length and color is consistent with that of A.C.. The title of the image file is: 10706563_863785953655045_1902793332_n.jpg. Based on a forensic examination of the file, it appears to have been created on or about September 22, 2014, and saved on the thumb drive on or about June 8, 2015.

11. FBI agents seized other electronic devices during the execution of the search. These devices are currently undergoing forensic examination.

12. In the course of speaking with one of ARROYO's relatives, FBI agents learned that the Forest Hills Address's Internet service was provided by Time Warner Cable / Roadrunner ("TWC"). This individual further stated that the TWC service was in her name.

13. In the course of speaking with one of ARROYO's relatives, FBI agents learned that ARROYO was at work. FBI agents located ARROYO at his place of employment in Queens. ARROYO agreed to be interviewed by FBI agents in an FBI automobile.

14. Agents advised the defendant of his Miranda rights. The defendant stated that he understood his rights, verbally waived his Miranda rights, and indicated that he wanted to speak to agents without a lawyer present. The interview was recorded by one of the agents present.

15. The defendant subsequently stated, in sum and substance, that he resided at the Forest Hills Address. The defendant further stated that he had asked A.C. to send him pornographic images and that he had received pornographic images of A.C. from A.C. via the Internet. The defendant further stated that he had communicated threats to A.C. via the Internet to the effect that he would post one or more pornographic images of A.C. if she were to terminate her relationship with the defendant.

16. FBI agents then placed the defendant under arrest.

WHEREFORE, your deponent respectfully requests that the defendant CHRISTOPHER ARROYO, be dealt with according to law.

STACY SHAHRANI
Special Agent
Federal Bureau of Investigation

Sworn to before me this
25th day of February, 2016

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

JAP:KDE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X
IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS 10520 66TH AVENUE, APARTMENT 6A, FOREST HILLS, NEW YORK 11375
- X

16M 144

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

EASTERN DISTRICT OF NEW YORK, SS:

LESLIE ADAMCZYK, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

1. Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 10520 66th Avenue, Apartment 6A, Forest Hills, New York 11375 (the "PREMISES"), further described in Attachment A to this affidavit, the items described in Attachment B to this affidavit, including computers, cellular telephones, electronic media, gaming systems and other items, all of which constitute evidence or instrumentalities of the offenses of or activities relating to: communications containing threats to injure the reputation of another, with the intent to extort from that person things of value, that is, images of a minor person in various states of undress, naked and engaging in sexually explicit conduct, in violation of 18 U.S.C. § 875(d); sexual exploitation of children in violation of 18 U.S.C. § 2251(a); material constituting or containing child pornography, in violation of 18 U.S.C. § 2252 and 2252A; harassment and intimidation using an interactive

computer service and facility of interstate commerce, to engage in a course of conduct that caused substantial emotional distress, in violation of 18 U.S.C. § 2261A(2)(B).

The source of your deponent's information and the grounds for her belief are as follows:[1]

2. I have been a Special Agent with the FBI since August 2012 and am currently assigned to the New York Office. Since October 2014, I have been assigned to a Crimes Against Children squad and have investigated violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through classroom training and daily work conducting these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities. As part of my responsibilities, I have been involved in the investigation of numerous child pornography ("CP") cases and have reviewed thousands of photographs depicting minors (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor. I am also a member of the Eastern District of New York Project Safe Childhood Task Force.

3. I am familiar with the facts and circumstances of this investigation from, among other sources, my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement

---

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

personnel concerning the creation, distribution, and proliferation of CP. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

I. DEFINITIONS

4. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct" and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[2]

c. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

d. The term "IP Address" or "Internet Protocol Address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0–255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other

---

[2] *See also Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

computers have dynamic — that is, frequently changed — IP addresses.

e. The term "Internet" refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. The term "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

g. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

h. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict

> access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

II. PROBABLE CAUSE

A. A.C. and Arroyo Relationship

5. In June 2015, an FBI Special Agent interviewed a female minor born on June 4, 2000, whose initials are A.C. A.C. provided the following information: in 2012, A.C. met an individual that identified himself as a teenage boy through a video game played on the Xbox gaming system called Halo Reach. Halo Reach allows the users of the game to communicate with other users through the Internet through online communication services provided by Microsoft Corporation. During their relationship, the individual who communicated with A.C. used the "gamer tags," or usernames chrissnake119 and chrissnake119x.

6. After their initial communication, A.C. and the individual continued to communicate through Halo Reach, the telephone, and through other services, such as Facebook ("FB") and Skype. A.C. and the individual began an on-line dating relationship.

7. The individual told A.C. that his name was CHRISTOPHER ARROYO, and that he lived in New York, New York. A.C. and ARROYO frequently communicated over FB. When ARROYO and A.C. first met, ARROYO used the FB profile name Christopher

Arroyo, but he later changed his profile name to Leon Mike. A.C. was aware that ARROYO's mother's FB profile name was Debbie Medina. A.C. positively identified to two pictures of ARROYO from the Christopher Arroyo FB profile and Debbie Medina's FB profile.

8. A.C. initially told ARROYO that she was 13 years old. ARROYO initially told her that he was 17 years of age. A.C. later admitted to ARROYO that she was 12 years old and he admitted to her he was really 23 years old. At one point in their relationship, ARROYO said age did not matter to him.

9. Approximately ten (10) months into their relationship, ARROYO asked A.C. to send him a picture of her body. She sent ARROYO a FB message with a picture of her upper body with her bra on. After the initial picture was sent, ARROYO began to ask A.C. for additional pictures of her body in various stages of undress. ARROYO described what poses he wanted and sent A.C. pictures of other people in those poses as examples of what he wanted. ARROYO also sent A.C. a picture of his penis. ARROYO frequently asked for pictures of A.C.'s bare breasts and of her bare lower body, bent over, taken from behind. A.C. sent ARROYO approximately 15 digital images over the Internet, at his demand, over a two year time period, including pictures of her masturbating. A.C. and ARROYO also communicated over video on Skype. At ARROYO's request, they both masturbated while on the video session.

10. If A.C. refused to take pictures for him or took pictures without her face in view, ARROYO would get angry with A.C. For instance, ARROYO yelled at A.C., in sum and substance and in part, "you don't love me if you don't do this," "I'm going to kill myself if you don't do this," and threatened that he would do something about it if she refused to send the pictures.

B. Threats and Harassment

11. Approximately one year into their relationship, A.C. attempted to break up with ARROYO. ARROYO told A.C. that if she broke up with him and stopped sending him pictures, he would post the pictures A.C. had sent him on the Internet and make A.C. look like a "slut." ARROYO also threatened to send people to her house to help her take the pictures. Due to the threats, A.C. continued to date him.

12. In June of 2014, A.C. tried to break up with ARROYO again. A.C. started to receive harassing messages from people on-line telling her she had to re-establish contact with ARROYO and date him again or else they would post her graphic photographs all over the Internet and tell her parents. A.C. was forced to start dating ARROYO again due to the harassment. When she refused to send additional pictures, he said he would make the harassers make her love him again.

13. In January of 2015, A.C. broke up with ARROYO for good because of his demands for graphic photographs. After this point, A.C. started receiving messages from different individuals, primarily through numerous FB accounts, harassing her and telling her to re-establish contact with ARROYO and date him again. Some of the pictures she had sent to ARROYO were then sent electronically through FB to A.C.'s friend, [another minor whose initials are] R.Z. Fictitious FB accounts were also created in the name of A.C. and her sister, whose initials are S.C. The fictitious FB accounts displayed derogatory messages and photographs of A.C. and contacted A.C.'s friends and family in order to ruin A.C.'s reputation and get her into trouble with her parents.

14. The individuals who harassed A.C. during this period used FB profile names including David Smith, Mang Kanor, Cassie Beauty Umbreon Makala, Lauren Cruz and Leon Mike. As noted above, ARROYO used the FB profile Leon Mike early in his relationship with A.C. Despite this harassment, A.C. refused to date ARROYO anymore.

15. On or about March 2 and 3, 2015, A.C. received messages on her XBox account from the gamertag YouWillSufferxx. YouWillSufferxx told A.C., in sum and substance and in part, that if she did not start talking again, he/she would tell A.C.'s mother what A.C. had done and A.C. would be forced to live a restricted life. The message also indicated that if A.C. does not reestablish contact with "Chris" and he therefore commits suicide, YouWillSufferxx would continue to harass A.C. for a long time.

16. On or about March 3, 2015, A.C. received messages on her Xbox account from the gamer tag TermedRegent872. TermedRegent872 told A.C., in sum and substance, that he/she found pictures of her and he/she did not know A.C. "shaved." TermedRegent872 told A.C. if she did not talk to "Chris," he/she would post the pictures on Facebook, Twitter, Twitch and other social media sites. TermedRegent872 told A.C. she would never be free unless she talked to Chris again.

17. On or around March 28, 2015, A.C. received FB messages from a user with the profile Lauren Cruz. Cruz told A.C., in sum and substance, that she found dark secrets about A.C. that her mother would be "pissed" about. Cruz told A.C. to talk to Chris now or she would make A.C.'s years in high school years unpleasant. Cruz said that she had been busy making A.C. "famous" and A.C. better reply to her message or she would do something A.C.

would not like. Cruz told A.C. that if she blocked her, she would tell her mother a dark secret. Cruz then said anything posted on DeviantART was art, not "porn."

18. After reading the messages, A.C. and her mother, whose initials are K.C., searched the social media site named DeviantART for postings about A.C. A.C. and K.C. located accounts on DeviantART with the profile names BlazingOrichalcum, Pikachu437, and one with the initials "A.C." The profiles all mentioned A.C.'s name. While A.C. and ARROYO were dating, ARROYO's username on "Kik," an Internet-based messaging application, was BlazingOrichalcum. The profile picture for the A.C. account was a picture of A.C's upper body with her hair covering her breasts.

19. The DeviantART profile Pikachu437 has a post saying the bullying of A.C. would continue until A.C. talked to ARROYO again. One of A.C.'s previous gamer tags on Xbox was Pikachu436.

20. An Internet search of A.C.'s name using a publically available search engine revealed the following: the same picture of A.C.'s upper body as well as another picture of A.C. in her bra and underwear were on the DeviantART website. A.C. recognized these pictures as pictures A.C. sent to ARROYO. Both of the filenames for these pictures included A.C.'s full name. Both pictures were posted by an individual with the user name frillist.

21. Through additional Internet searches, A.C. discovered that several of the graphic pictures she had sent to ARROYO were posted on multiple different social media accounts including, but not limited to, FB, DeviantART, Pinterest, Twitch, Imgur, Google Plus, and Twitter. Many of the profile names for the accounts that posted these pictures were variations of A.C.'s full name. The pictures were of A.C. in various states of undress, including

pictures of her bare breasts and of her lower body in a sexually explicit pose. For instance, in one of the pictures of A.C., she is in a sexually explicit pose on her hands and knees wearing a shirt and g-string underwear. There was a mirror behind her so the picture captured her pubic area.

22. In addition, in early 2015, A.C. received a Skype message from moonlightbeautyumbreon that told A.C. she should talk or else every picture would be posted and A.C. would be exposed. Similarly, A.C. received a message on her Twitter account from Cassie Makala @BeautyUmbreon. The message said @ChrisOrichalcum was joining in the fun and A.C. was screwed.

23. K.C. recalled that around April of 2015, one of the messages A.C. received through FB told her that she had five days to re-contact ARROYO or else the FB user would post pictures and would ruin her (A.C.'s) life and make people think she was a "whore." The individual also said he/she had already got one girl to kill herself. A.C. and K.C. stopped responding to the harassing FB messages, but continued to search A.C.'s name on an Internet search engine to find any additional pictures.

24. On or about September 10, 2015, the account profile AlanasFault on DeviantART posted that A.C. was "going down" and the poster was "taking [A.C.] on."

25. Further, in 2015, while searching the Internet for pictures of her daughter, K.C. found an account with A.C.'s name on a photograph-sharing website called Imgur that posted a picture of her bare breasts and a picture of A.C. bending over so the picture captured her vaginal and butt area. In addition, K.C. located an account with user name "[A]_[C]" on a website called Twitch. On this account, there were graphic pictures of A.C. and posts that stated,

in sum and substance and in part, that A.C. was a "backstabber" and that she loved to take pictures of herself to gain attention and that the pictures were legal, so she stop complaining.

26. As of at least October 7, 2015, K.C. continued to find the sexually explicit picture of A.C. on her hands and knees, as described above, on es.pinterest.com and Tumblr, two additional Internet-based photographs sharing websites, posted by an individual with the user name of A.C.'s full name.

C. Law Enforcement Involvement

27. On or about March 30, 2015, the National Center for Missing and Exploited Children (NCMEC) received a Cyber Tipline report from DeviantART Inc. (DeviantART). DeviantART reported that username with the full name of A.C. (separated by a hyphen) had uploaded nude photographs of a minor, one of which appeared to be A.C's nude upper body, including her face, but with her hair covering her breasts ("Photograph 1"). The other photograph reported by DeviantART did not have a face in it, but it showed a nude female upper body with the breasts covered by the female's arm and hair. The curtains in the background appeared to be the same as the curtains in the background of the first picture of A.C. The filename associated with the latter picture was "[A.C.]'s glamorous hair shine." The login IP address of the user was 67.243.177.202, with a date and time of March 30, 2015 at 01:06:00 UTC.

28. On or about May 26, 2015, NCMEC received a report from Twitter, Inc. (Twitter) regarding pictures uploaded by user name Pikachu437x. The uploaded pictures included a picture of A.C. taking a picture of her back side in a mirror while wearing only underwear. Another picture was Photograph 1. Twitter reported that user name Pikachu437x

had a registration and on May 5, 2015 at 04:04:40 UTC and May 21, 2015 at 08:13:14 UTC, a login IP address of 98.14.78.38.

29. On or about May 29, 2015, NCMEC received a report from Twitter regarding pictures uploaded by user name pikachu437xyz. The uploaded pictures included the graphic picture of A.C. in a sexually explicit pose on her hands and knees as described above. Twitter reported that user name pikachu437xyz had a registration and on May 27, 2015 at 08:13:59 UTC and May 29, 2015 at 06:54:31 UTC a login IP address of 98.14.78.38.

30. On or about May 30, 2015, NCMEC received a report from Twitter regarding pictures uploaded by user name with A.C.'s full name, separated by an underscore. The photograph appeared to be Photograph 1. Twitter reported this user had a registration and on May 22, 2015 at 06:49:05 UTC and May 29, 2015 at 06:47:57 UTC, a login IP address of 98.14.78.38.

31. On or about May 30, 2015, NCMEC received a report from Twitter regarding pictures uploaded by user name DeadAndUgly69. The uploaded pictures included the picture of A.C. in a sexually explicit pose. Twitter reported that user name DeadAndUgly69 had a login IP address of 98.14.78.38, on May 27, 2015 at 03:04:48 UTC and May 30, 2015 at 17:56:37 UTC.

32. On or about June 23, 2015, in response to an administrative subpoena, DeviantART provided subscriber information on user names [A]-[C], frillist and BlazingOrichalcum. The IP logs for the three accounts showed that all three accounts had connected to DeviantART from IP address 98.14.78.38 on different occasions. In addition,

BlazingOrichalcum and [A]-[C] had also used IP address 67.243.177.202 to log on to the website.

33. On or about June 23, 2015, in response to an administrative subpoena, Kik Interactive, Inc. (Kik) provided subscriber information on user name BlazingOrichalcum. The name on the account was CHRISTOPHER ARROYO and the user had connected to Kik through IP address 98.14.78.38 on May 22, 2015 at 10:38:44 EDT.

34. As described above, K.C. found on Imgur appeared a picture of A.C.'s bare breasts and a picture of A.C. bending over so the picture captured her vaginal and butt area. In response to an administrative subpoena, Imgur provided records indicating that the account user who posted these photographs had accessed the Imgur site using IP address 98.14.78.38 on June 5, 2015 at 03:26 UTC.

35. On or about July 14, 2015, in response to an administrative subpoena, Skype Communications (Skype) provided subscriber information for username moonlightbeautyumbreon. The user had created the account on Skype using IP address 98.14.78.38 on May 11, 2015 at 09:51:975 UTC.

36. In addition, Twitch Interactive, Inc. has provided records pursuant to a subpoena indicating that the user who, as described above, had stated, among other things, that A.C. was a backstabber, connected to the Twitch site using IP address 98.14.78.38 on June 19, 2015.

37. Similarly, in response to an administrative subpoena, Facebook, Inc. (FB) provided subscriber records for user names David Smith, Mang Kanor, Cassie BeautyUmbreon

Makala, Leon Mike and Christopher Arroyo. All of the users had accessed FB using IP address 67.243.177.202 on multiple occasions.

38. Using a publically available IP locator search site, it was determined both IP addresses 98.14.78.38 and 67.243.177.202 belonged to Time Warner Cable/Road Runner (TWC).

39. In response to an administrative subpoena, TWC provided subscriber records for the user of IP addresses 98.14.78.38 and 67.243.177.202. Based on specific dates and times identified during the investigation which coincided with a suspect conducting on-line activity, six different dates and times between May 1, 2015 and June 1, 2015 for IP address 98.14.78.38 and five specific dates and times between March 28, 2015 and April 1, 2015 for IP address 67.243.177.202 were requested. At the specified times, both of the IP addresses were assigned to an account belonging to DEBBIE FARFAN-MEDINA, located at 10520 66th Avenue, Apt 6A, Forest Hills, NY 11375. Updated administrative subpoenas as of approximately February 3, 2016, revealed that the two above IP addresses (98.14.78.38 and 67.243.177.202) are still assigned to an account belonging to DEBBIE FARFAN-MEDINA, located at 10520 66th Avenue, Apt 6A, Forest Hills, NY 11375.

40. Based on a search conducted on Accurint, a database available to law enforcement to conduct searches on people and properties, CHRISTOPHER ARROYO was a resident at 10520 66th Avenue, Apt 6A, Forest Hills, NY 11375. A search of the New York Drivers and Motor Vehicles database identified ARROYO as residing at that address. The Driver's License photograph of ARROYO appeared to match the photographs of ARROYO on FB previously identified by A.C.

II. THE PREMISES

41. The PREMISES is located on the sixth floor of a multi-story apartment building. The entrance to the building has a main door which is glass and only accessible by being buzzed in by a resident. The door of the PREMISES is on the sixth floor, is blue in color, and identified as "6A".

42. On January 27, 2016, a Special Agent acting in an undercover capacity (UCE) knocked on the door of the PREMISES. Two males answered the door and identified themselves as Evan Medina and Christopher Arroyo. Arroyo further informed the UCE that Deborah Medina resides in the apartment.

III. CHARACTERISTICS OF INDIVIDUALS INVOLVED IN THE DISTRIBUTION OF CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

43. Based upon my knowledge, experience, and training in child pornography and child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that there are certain characteristics common to many individuals involved in the possession and distribution of child pornography and the exploitation of children. Those who possess and distribute child pornography and exploit children:

a. Often receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity;

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media.

Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner or to demonstrate the desired sexual acts;

c. May possess and maintain hard copies of child pornographic material, such as pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Some of these individuals retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica and videotapes for many years;

d. Often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly;

e. Often possess multiple digital devices, such as desktop and laptop computers, smart phones, tablet computers, etc. and multiple storage devices, such as flash drives and memory, external hard drives, CDs, etc. which are used to access, distribute, and store child pornography. Many of these items are small, some flash memory devices are smaller than a postage stamp, and easily concealed;

f. Tend to keep their older devices even after upgrading to newer technology. The older devices, along with the items stored on them, are often still accessible;

g. May utilize online/remote storage services to store, access, and distribute child pornography. The content stored on online storage services may accessible through the subject's computer while it is logged in, but may be difficult to obtain once the computer is turned off;

h. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence

as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography; and

i. Prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

44. Based on my training and experience in child exploitation matters, I have seen the number of incidents of child exploitation involving individuals enticing, harassing, threatening or coercing minors to produce images of child pornography have risen dramatically in the past few years. One of the factors is that children have increasing access to Internet connected devices and messaging applications. The individuals frequently befriend and groom the minor through a social media site or messaging application and establish a relationship. Once a relationship has been established, the individual requests that the minor produce a picture/digital image that would embarrass the minor, or get him/her into trouble, if friends or family were to see it. If the minor refuses, the individual frequently uses ploys, such as telling the minor that if he/she loved the individual, he/she will do it, or threatening to tell the minor's parents about his/her online activities. The first picture is usually less revealing than future pictures. Once the first picture is received, the individual uses that picture to threaten the minor into producing additional child pornographic pictures or videos. The minors frequently feel that they have no other choice but to comply due to the threats and harassment. The individuals engaging in these behaviors frequently are victimizing several different minors at the same time.

IV. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

45. As described above, this application seeks permission to search for the items described more fully in Attachment B for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Federal Rule of Criminal Procedure 41(e)(2)(B).

46. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file

system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

47. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

48. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

50. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that ~~that~~ it is reasonably likely ~~possible~~ that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

V. CONCLUSION

51. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes. Accordingly, a search warrant is requested.

52. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 10520 66TH AVENUE, APARTMENT 6A, FOREST HILLS, NEW YORK 11375.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

LESLIE ADAMCZYK
Special Agent
Federal Bureau of Investigation

Sworn to before me this 22nd day of February 2016

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

The property to be searched is 10520 66TH AVENUE, APARTMENT 6A, FOREST HILLS, NEW YORK 11375, further described as an apartment located on the sixth floor of a multi-story apartment building. The entrance to the building is buzzer controlled. The door to the PREMISES is blue in color and is identified with the number "6A".

ATTACHMENT B
Property to be Seized

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of 18 U.S.C. §§ 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B):

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B), in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 875(d), 2251(a),

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

2252, 2252A, and 2261A(2)(B). All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B), including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

---

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

16. Records and things evidencing the use of the Internet Protocol addresses 98.14.78.38 and 67.243.177.20, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES KNOWN AND DESCRIBED AS 10520 66TH AVENUE, APARTMENT 6A, FOREST HILLS, NEW YORK 11375

Case No. 16M1447

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 7, 2016 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ___ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ___

Date and time issued: 2-22-16 4:30 PM

Judge's signature

City and state: Brooklyn, New York Hon. Steven M. Gold U.S.M.J.
Printed name and title

ATTACHMENT A
Property to Be Searched

The property to be searched is 10520 66TH AVENUE, APARTMENT 6A, FOREST HILLS, NEW YORK 11375, further described as an apartment located on the sixth floor of a multi-story apartment building. The entrance to the building is buzzer controlled. The door to the PREMISES is blue in color and is identified with the number "6A".

ATTACHMENT B
Property to be Seized

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of 18 U.S.C. §§ 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B):

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B), in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 875(d), 2251(a),

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

2252, 2252A, and 2261A(2)(B). All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 875(d), 2251(a), 2252, 2252A, and 2261A(2)(B), including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

---

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

16. Records and things evidencing the use of the Internet Protocol addresses 98.14.78.38 and 67.243.177.20, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.